UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 09/754,635 | 01/04/2001 | Walter Einfeldt | PHDE000003 | 3606 |

24737 7590 10/08/2004

PHILIPS INTELLECTUAL PROPERTY & STANDARDS
P.O. BOX 3001
BRIARCLIFF MANOR, NY 10510

| EXAMINER | |
|---|---|
| SMITHERS, MATTHEW | |

| ART UNIT | PAPER NUMBER |
|---|---|
| 2137 | |

DATE MAILED: 10/08/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

| Office Action Summary | Application No. | Applicant(s) | |
|---|---|---|---|
| | 09/754,635 | EINFELDT ET AL. | |
| | Examiner | Art Unit | |
| | Matthew B Smithers | 2137 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *04 January 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☒ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *04012001; 21032001*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

## DETAILED ACTION

### *Priority*

Acknowledgment is made of applicant's claim for foreign priority based on an application filed in Germany on 08 January 2000. It is noted, however, that applicant has not filed a certified copy of the 10000502.0 application as required by 35 U.S.C. 119(b). More specifically, an English language translation of the German document is required.

### *Information Disclosure Statement*

The information disclosure statements filed 04 January 2001 and 21 March 2001 have been placed in the application file and the information referred to therein has been considered as to the merits.

### *Claim Objections*

Claims 5-20 are objected to under 37 CFR 1.75(c), as being of improper dependent form for failing to further limit the subject matter of a previous claim. Applicant is required to cancel the claim(s), or amend the claim(s) to place the claim(s) in proper dependent form, or rewrite the claim(s) in independent form. More specifically, claims 5-20 are multiple dependent claims depending from multiple dependent claim 4. According to MPEP 608.01(n) B.4., the above claims are unacceptable multiple dependent claims.

### *Claim Rejections - 35 USC § 112*

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 5-20 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Each claim refers back to a multiple dependent claim. All multiple dependent claims incorporate the limitations or elements of the claims they depend from and forms a set of alternative embodiments of the claimed invention. As such any subsequent multiple dependent claim that refer back to a first multiple dependent claim take on the limitations or elements of each of the alternatives formed from the first multiple dependent claim. This type of situation creates multiple alternative sets from the single alternative sets formed by the first multiple dependent claim and as such causes the claims to be indefinite for failing to particularly point out and distinctly claim the scope of the subject matter applicant regards as their invention. See MPEP 608.01(n).

### *Claim Rejections - 35 USC § 102*

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1-20 are rejected under 35 U.S.C. 102(b) as being anticipated by U.S. patent 4,799,259 granted to Ogrodski.

Regarding claim 1, Ogrodski meets the limitations as follows:

"A method of generating a random number sequence, particularly in a chip card or smart card, characterized by the steps of

(a) scanning the outputs of Nosz independent frequency oscillators and buffering corresponding Nosz output signals of the Nosz frequency oscillators at each clock of a clock signal from an external clock signal source,

(b) applying the buffered signals of step (a) to a logic operation assigning a predetermined output value to the Nosz buffered signals as input values,

(c) generating the parity of a predetermined number Nlog of output values of step (b) at each $Nlog^{th}$ clock of the external clock signal,

(d) storing a predetermined number Nz of parity numbers in a random number register, and

(e) reading all of the Nz*Nlog clocks of the clock signal as a random number from the random-number register." see Abstract, column 8, line 45 to column 10, line 7.

Regarding claim 2, Ogrodski meets the limitations as follows:

"A method as claimed in claim 1, characterized in that the frequency of at least one frequency oscillator is changed and/or modulated in dependence upon an MSB (Most Significant Bit) of a signature register." see column 9, line 64 to column 10, line 7.

Regarding claim 3, Ogrodski meets the limitations as follows:

"A method as claimed in claim 2, characterized in that the frequency of the

changed or modulated frequency oscillator is switched between > 20 MHz and > 40 MHz in dependence upon the MSB of the signature register." see column 9, line 64 to column 10, line 7.

Regarding claim 4, Ogrodski meets the limitations as follows:

"A method as claimed in any one of the preceding claims, characterized in that the frequency of at least one frequency oscillator is selected to be > 30 MHz." see column 9, lines 55-63.

Regarding claim 5, Ogrodski meets the limitations as follows:

"A method as claimed in any one of the preceding claims, characterized in that the frequency oscillators are voltage-controlled or current-controlled." see column 2, lines 40-61.

Regarding claim 6, Ogrodski meets the limitations as follows:

"A method as claimed in any one of the preceding claims, characterized in that in step (a), the output signals of the two frequency oscillators are buffered in a respective flip-flop, particularly a delay flip-flop (D-FIF)." see column 2, lines 45-51.

Regarding claim 7, Ogrodski meets the limitations as follows:

"A method as claimed in any one of the preceding claims, characterized in that in step (c) the logic operation is an AND operation (AND), an OR operation (OR), a NOR operation (NOR), an Exclusive-OR operation (XOR), a NAND operation (NAND) or an Exclusive-NOR operation (XNOR)." see column 2, lines 45-51; column 3, lines 38-55 and column 4, lines 34-50.

Regarding claim 8, Ogrodski meets the limitations as follows:

"A method as claimed in any one of the preceding claims, characterized in that the frequencies of the Nosz frequency oscillators are selected to be such that no frequency of a frequency oscillator is an integral multiple of another frequency oscillator or of the external clock signal." see column 9, lines 33-38.

Regarding claim 9, Ogrodski meets the limitations as follows:

"A method as claimed in any one of the preceding claims, characterized in that Nosz is an integer which is larger than or equal to 1, particularly Nosz = 2." see column 8, lines 9-21.

Regarding claim 10, Ogrodski meets the limitations as follows:

"A method as claimed in any one of the preceding claims, characterized in that Nlog and Nz are integers which are larger than or equal to 1." see column 8, lines 9-21.

Regarding claim 11, Ogrodski meets the limitations as follows:

"A random-number generator, particularly for a chip card or a smart card, particularly for performing a method as claimed in any one of the preceding claims, characterized by a predetermined number Nosz, of mutually independent frequency oscillators (10, 12), a predetermined number Nosz of flip-flops (14, 16), in which an output (26) of a frequency oscillator (10, 12) is connected to an input D (30) of a flip-flop (14, 16), a logic circuit element (18) receiving outputs Q (32) of the flip-flops (14, 16) as input values (36, 38) and, in accordance with a predetermined logic operation, assigns an output value (40) to these input values (36, 38), a parity circuit (20) determining the parity of a predetermined number Nlog of output values (40) from the logic circuit element (18), a random-number register (22) which buffers a predetermined number Nz of parity

numbers (44) from the parity circuit (20) and supplies them as Nz bit random number, and an input (58) for an external clock signal source which clocks the flip-flops (14, 16), the parity circuit (20) and the random-number register (22)." see Abstract, column 8, line 45 to column 10, line 7.

Regarding claim 12, Ogrodski meets the limitations as follows:

"A random-number generator as claimed in claim 11, characterized in that at least one frequency oscillator (10) is connected to an output of a signature register which applies an MSB (Most Significant Bit) (29) to the frequency oscillator, the frequency of the frequency oscillator (10) changing in dependence upon the MSB (29) of the signature register." see column 9, line 64 to column 10, line 7.

Regarding claim 13, Ogrodski meets the limitations as follows:

"A random-number generator as claimed in claim 12, characterized in that the frequency oscillator (10) connected to the signature register is formed in such a way that it switches its frequency between > 20 MHz and > 40 MHz in dependence upon the MSB (29) of the signature register." see column 9, lines 55-63 and column 9, line 64 to column 10, line 7.

Regarding claim 14, Ogrodski meets the limitations as follows:

"A random-number generator as claimed in any one of claims 11 to 13, characterized in that the frequency of at least one frequency oscillator (12) is > 30 MHz." see column 9, lines 55-63.

Regarding claim 15, Ogrodski meets the limitations as follows:

"A random-number generator as claimed in any one of claims 11 to 14, characterized in that the frequency oscillators (10, 12) are formed as voltage-controlled or current-controlled frequency oscillators." see column 2, lines 40-61.

Regarding claim 16, Ogrodski meets the limitations as follows:

"A random-number generator as claimed in any one of claims 11 to 15, characterized in that at least one flip-flop (14, 16) is formed as a delay flip-flop (D-F/F) ." see column 2, lines 45-51.

Regarding claim 17, Ogrodski meets the limitations as follows:

"A random-number generator as claimed in any one of claims 11 to 16, characterized in that the logic circuit element (18) is an AND element (AND), an OR element (OR), a NOR element (NOR), an Exclusive-OR element (XOR), a NAND element (NAND) or an Exclusive-NOR element (XNOR) ." see column 2, lines 45-51; column 3, lines 38-55 and column 4, lines 34-50.see column 8, lines 9-21; column 9, lines 33-38.

Regarding claim 18, Ogrodski meets the limitations as follows:

"A random-number generator as claimed in any one of claims 11 to 17, characterized in that the Nosz frequency oscillators (10, 12) are formed in such a way that no frequency of a frequency oscillator (10, 12) is an integral multiple of another frequency oscillator (10,12) or of the external clock signal (58)." see column 9, lines 33-38.

Regarding claim 19, Ogrodski meets the limitations as follows:

"A random-number generator as claimed in any one of claims 11 to 18, characterized in that Nosz is an integer which is larger than or equal to 1, particularly Nosz =2." see column 8, lines 9-21.

Regarding claim 20, Ogrodski meets the limitations as follows:

"A random-number generator as claimed in any one of claims 11 to 19, characterized in that Nlog and Nz are integers which are larger than or equal to 1." see column 8, lines 9-21.

***Claim Rejections - 35 USC § 102***

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1-4, 7,8 11-14, 17 and 18 are rejected under 35 U.S.C. 102(e) as being anticipated by U.S. 6,714,955 granted to Le Quere.

Regarding claim 1, Le Quere meets the limitations as follows:

"A method of generating a random number sequence, particularly in a chip card or smart card, characterized by the steps of

(a) scanning the outputs of Nosz independent frequency oscillators and buffering corresponding Nosz output signals of the Nosz frequency oscillators at each clock of a clock signal from an external clock signal source," see column 4, lines 25-28

"(b) applying the buffered signals of step (a) to a logic operation assigning a predetermined output value to the Nosz buffered signals as input values," see column 4, lines 35-38.

"(c) generating the parity of a predetermined number Nlog of output values of step (b) at each Nlog$^{th}$ clock of the external clock signal,

(d) storing a predetermined number Nz of parity numbers in a random number register, and

(e) reading all of the Nz*Nlog clocks of the clock signal as a random number from the random-number register." see column 3, line 26 to column 6, line 25.

Regarding claim 2, Le Quere meets the limitations as follows:

"A method as claimed in claim 1, characterized in that the frequency of at least one frequency oscillator is changed and/or modulated in dependence upon an MSB (Most Significant Bit) of a signature register." see column 5, lines 26-37.

Regarding claim 3, Le Quere meets the limitations as follows:

"A method as claimed in claim 2, characterized in that the frequency of the changed or modulated frequency oscillator is switched between > 20 MHz and > 40 MHz in dependence upon the MSB of the signature register." see column 3, line 26 to column 6, line 25.

Regarding claim 4, Le Quere meets the limitations as follows:

"A method as claimed in any one of the preceding claims, characterized in that the frequency of at least one frequency oscillator is selected to be > 30 MHz." see Figure 2, element 8.

Regarding claim 7, Le Quere meets the limitations as follows:

"A method as claimed in any one of the preceding claims, characterized in that in step (c) the logic operation is an AND operation (AND), an OR operation (OR), a NOR operation (NOR), an Exclusive-OR operation (XOR), a NAND operation (NAND) or an Exclusive-NOR operation (XNOR)." see column 5, lines 34-37.

Regarding claim 8, Le Quere meets the limitations as follows:

"A method as claimed in any one of the preceding claims, characterized in that the frequencies of the Nosz frequency oscillators are selected to be such that no frequency of a frequency oscillator is an integral multiple of another frequency oscillator or of the external clock signal." see column 5, lines 26-30.

Regarding claim 11, Le Quere meets the limitations as follows:

"A random-number generator, particularly for a chip card or a smart card, particularly for performing a method as claimed in any one of the preceding claims, characterized by a predetermined number Nosz, of mutually independent frequency oscillators (10, 12), a predetermined number Nosz of flip-flops (14, 16), in which an output (26) of a frequency oscillator (10, 12) is connected to an input D (30) of a flip-flop (14, 16), a logic circuit element (18) receiving outputs Q (32) of the flip-flops (14, 16) as input values (36, 38) and, in accordance with a predetermined logic operation, assigns an output value (40) to these input values (36, 38), a parity circuit (20) determining the parity of a predetermined number Nlog of output values (40) from the logic circuit element (18), a random-number register (22) which buffers a predetermined number Nz of parity numbers (44) from the parity circuit (20) and supplies them as Nz bit random number,

and an input (58) for an external clock signal source which clocks the flip-flops (14, 16), the parity circuit (20) and the random-number register (22)." see column 3, line 26 to column 6, line 25.

Regarding claim 12, Le Quere meets the limitations as follows:

"A random-number generator as claimed in claim 11, characterized in that at least one frequency oscillator (10) is connected to an output of a signature register which applies an MSB (Most Significant Bit) (29) to the frequency oscillator, the frequency of the frequency oscillator (10) changing in dependence: upon the MSB (29) of the signature register." see column 3, line 26 to column 6, line 25.

Regarding claim 13, Le Quere meets the limitations as follows:

"A random-number generator as claimed in claim 12, characterized in that the frequency oscillator (10) connected to the signature register is formed in such a way that it switches its frequency between > 20 MHz and > 40 MHz in dependence upon the MSB (29) of the signature register." see Figure 2.

Regarding claim 14, Le Quere meets the limitations as follows:

"A random-number generator as claimed in any one of claims 11 to 13, characterized in that the frequency of at least one frequency oscillator (12) is > 30 MHz." see Figure 2, element 8.

Regarding claim 17, Le Quere meets the limitations as follows:

"A random-number generator as claimed in any one of claims 11 to 16, characterized in that the logic circuit element (18) is an AND element (AND), an OR element (OR), a

NOR element (NOR), an Exclusive-OR element (XOR), a NAND element (NAND) or an Exclusive-NOR element (XNOR)." see column 5, lines 34-37.

Regarding claim 18, Le Quere meets the limitations as follows:

"A random-number generator as claimed in any one of claims 11 to 17, characterized in that the Nosz frequency oscillators (10, 12) are formed in such a way that no frequency of a frequency oscillator (10, 12) is an integral multiple of another frequency oscillator (10,12) or of the external clock signal (58)." see column 5, lines 26-30.

***Conclusion***

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

A. Bernstein et al (5,007,087) discloses a method for generating random numbers using chaos.

B. Takahashi (5,570,307) discloses an on-chip digital randomizer using flip-flops.

C. Gilley (5,781,458) discloses a method for generating random numbers using an oscillator circuit.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Matthew B Smithers whose telephone number is (703) 308-9293. The examiner can normally be reached on Monday-Friday (9:00-5:30) EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew T Caldwell can be reached on (703) 306-3036. The fax phone

number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Matthew B Smithers
Primary Examiner
Art Unit 2137